# BreachVector

Website Security Review

88

Target: northstar-finance.demo

Normalized URL: https://northstar-finance.demo
Completed: Mar 27, 2026, 3:31 PM
Origin: Seeded showcase

## Executive summary

Northstar Finance presents a mature external security baseline with HTTPS, redirect enforcement, and most critical hardening controls in place. The largest gap is the absence of a content security policy, which leaves browser-side protections weaker than the rest of the stack.

## Top findings

### MEDIUM - Content Security Policy is missing

The site does not publish a Content-Security-Policy header, so browsers have fewer constraints on where scripts, frames, and other resources can load from.

Remediation: Add a baseline Content-Security-Policy and tighten it over time, starting with default-src 'self' and explicit script/frame allowlists.

### INFO - Cookie posture is strong

Visible cookies include Secure, HttpOnly, and SameSite flags, which reduces exposure to common session handling mistakes.

Remediation: Keep these flags enforced across new session and preference cookies.

## Technical narrative

Transport security is well configured: HTTPS is reachable, HTTP redirects to HTTPS, and TLS validity looks healthy. The site would benefit most from client-side browser hardening via a Content-Security-Policy, while its current header and cookie posture already covers several common baselines.

## Remediation plan

### Immediate - Introduce a baseline CSP

Start with a conservative policy, test in report-only mode if needed, then enforce once third-party resources are explicitly allowlisted.

### Next sprint - Tune CSP for third-party tools

Audit analytics, payment, and support widgets so the policy stays specific and maintainable.

## Signal breakdown

HTTPS reachable: Yes
HTTP redirects to HTTPS: Yes
HTTPS status: 200
HTTP status: 301
TLS expiration: Nov 14, 2026, 12:00 PM
SPF: Present
DMARC: Present

# Plain-English notes

## HTTPS

HTTPS encrypts the connection between a visitor and your site so traffic cannot be read or altered in transit as easily.

## Content Security Policy

A content security policy tells the browser which scripts, frames, and external resources are allowed to run on the page.